

REMARKS

This Amendment serves as a submission accompanying a Request for Continued Examination (RCE) being filed herewith.

New claim 19 has been added. Claims 8 and 12 have been amended. No new matter has been added. Claims 8 to 19 are now pending. Applicants respectfully request reconsideration of the present application in view of this Response.

35 U.S.C. §112, first paragraph

In the earlier final Office Action, claim 12 was rejected under 35 U.S.C. §112, first paragraph, for lack of written description. While Applicants believe that claim 12 was amply described in the Specification, claim 12 has been amended above. The amendments to claim 12 are described in the Specification, e.g., at page 3, lines 32-33, and in originally filed Fig. 7. Applicants respectfully submit that claim 12 as written was supported by the Specification. Accordingly, Applicants respectfully submit that claim 12 as presented is fully supported by the written description in the Specification, and withdrawal of the rejection under 35 U.S.C. §112, first paragraph, is respectfully requested.

35 U.S.C. §103

In the earlier final Office Action, claims 8 to 18 were rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Patent No. 5,805,204 to Thompson (“Thompson reference”) in view of U.S. Patent No. 6,285,991 to Powar (“Powar reference”).

Applicants’ earlier remarks in other responses / amendments are incorporated herein by reference.

Applicants respectfully submit that claims 8 to 18 are allowable over the cited Thompson and Powar references.

The Thompson reference refers to an interactive video guide in which object code is transmitted to set-top decoder units located in customers’ homes. The Thompson reference appears to indicate that to send encrypted data, a random number is first generated by a program within the headend computer; and an appropriate imbedded key (the chosen key for the time period) is selected and loaded into the system specific algorithm. Apparently, the random number is encrypted using the DES algorithm which has been initialized and loaded with the appropriate key, producing a result which is the current system seed key. The seed key is then loaded into the system specific algorithm through which the actual transmitted data is passed. The initial random number is transmitted in clear text along with the encrypted data. When the data is received by a subscriber unit, a period identifier may be used to identify which of the keys

previously and securely imbedded into the smart card will be used for the decryption process. This key must be the same one used at the headend computer for the same time period.

The Powar reference refers to an interactive electronic account statement delivery system for using over the Internet. Specifically, the Powar reference refers to a system where the certification authority grants digital certificates to the certificated banks, which in turn grant digital certificates to billers and customers. Then, digital certificates form the basis for encryption and authentication of network communications, using public and private keys. The reference refers to the certificates as being stored as digital data on storage media of a customer's or biller's computer system, or contained in integrated circuit or chip cards physically issued to billers and customers.

In contrast, claim 8 is directed to a method for implementing an encryption system, including *generating a Vernam key via a symmetrical cipher*, the generating being aided by using a secret key and a variable parameter, the Vernam key having a length that is equal to a length of a message to be protected, *the secret key having a defined key length, the variable parameter having a length which is a function of the defined key length*. Via a Vernam key, the message is encrypted using logic operations of a Vernam cipher. *And, from a sending point to a receiving point, the secret key and the variable parameter are communicated via a secure channel separate from a message-transmission path*. The Vernam key is regenerated, and the message is decrypted using the regenerated Vernam key. A storage space and one of a symmetrical cipher and the asymmetrical cipher are installed in a crypto-module, the crypto-module being separate from an encryptor; and performing encryption operations via the Vernam cipher in the encryptor.

Neither of the references, alone or in combination, appear to teach or describe such a system in which a secret key and a variable parameter are devised and then transmitted via a secure channel separate from a message-transmission path. Further, neither reference, alone or in combination, appear to teach or describe a Vernam key which is regenerated as in the present system after transmission, or installing a storage space and one of a symmetrical cipher and an asymmetrical cipher in a crypto-module, the crypto-module being separate from the encryptor, and performing encryption operations via the Vernam cipher in the encryptor.

Further, Applicants respectfully submit that the references are not combinable as one reference concerns itself with set-top devices which receive signals and the other reference concerns itself with an account delivery system, each of the systems concerning a different type of transmission and transmission of different types of data.

Accordingly, Applicants respectfully submit that the Thompson and Powar references in combination or alone do not teach or describe all of the features of claim 8. Allowance of claim 8 is respectfully requested.

Claims 9 to 14 depend from claim 8, those claims should be allowable for at least the same reasons as claim 8. Claims 15 and 18, as well as dependent claims 16 to 17, recite features analogous to those of claim 8, and should be allowable for essentially the same reasons as claim 8.

Accordingly, Applicants respectfully request the withdrawal of the rejection of claim 8 to 18 under 35 U.S.C. § 103(a) over the Thompson reference in view of the Powar reference.

CONCLUSION

For at least the foregoing reasons, Applicants respectfully submit that any outstanding rejections of claims 8 to 19 under 35 U.S.C. §§ 103(a), 112 have been overcome, and that all pending claims are in condition for allowance.

It is therefore respectfully requested that the rejections be reconsidered and withdrawn, and that the present application issue as early as possible.

Respectfully submitted,

Dated: July 28, 2009

By: /Linda Lecomte/
Linda Shudy Lecomte (Reg. No. 47,084)

CUSTOMER NO. 26646

KENYON & KENYON LLP
One Broadway
New York, New York 10004
(212) 425-7200